



INDIANA STATE DEPARTMENT OF HEALTH

---

Public Health Emergency Surveillance System

# PHIESS Transition Plan

INDIANA STATE DEPARTMENT OF HEALTH

# **PHESS Transition Plan**

---

Prepared by:  
The Regenstrief Institute  
1050 Wishard Boulevard  
Indianapolis, Indiana 46202-2872  
Phone 317.630.7400 • Fax 317.630.6962

---

# Table of Contents

<b>PHESSTransition Plan</b>	<b>1</b>
<b>I. Functional components</b>	<b>1</b>
<b>A. Secure Connectivity</b>	<b>2</b>
<b>B. HL7 Interface Engine</b>	<b>2</b>
<b>C. Message Queuing/Processing</b>	<b>2</b>
<b>D. System Maintenance</b>	<b>2</b>
<b>II. Transition Strategies</b>	<b>3</b>
<b>A. Non-INPC hospital transition</b>	<b>3</b>
<b>B. INPC hospital transition</b>	<b>4</b>
<b>III. Maintenance Tasks: Reconnection Process</b>	<b>4</b>
<b>A. Core source system components</b>	<b>4</b>
<b>B. Common modification</b>	<b>5</b>
<b>C. Reconnection tasks</b>	<b>5</b>
<b>D. Message Review</b>	<b>6</b>
<b>E. Re-establish Connectivity</b>	<b>7</b>
<b>F. Go Live – Establish Data Transfer</b>	<b>8</b>
<b>Appendix A: Frequently Asked Questions</b>	<b>9</b>
<b>Appendix B: Sample VPN Worksheet</b>	<b>13</b>

---



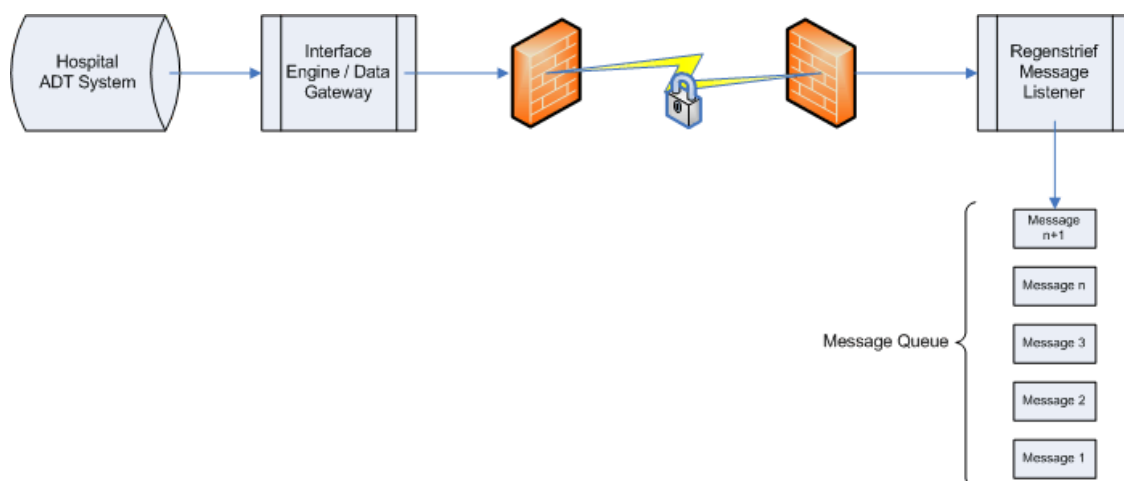
## PHESS Transition Plan

*Contractor will prepare and deliver to ISDH a transition plan, detailing how the Collection System could be transitioned to another vendor or ISDH for use and support. This transition plan will be delivered to ISDH within 30 days prior to the end of the Contract term.*

### ***I. Functional components***

The following are key operational components of the Indiana public health emergency surveillance system (PHESS) to be considered within this transition plan:

- Secure Connectivity
- HL7 Interface Engine
- Message Queuing/Processing
- System Maintenance



## **A. Secure Connectivity**

Hospitals that send data for the PHESS project must transmit data in a manner that protects the privacy and confidentiality of the data because it contains protected health information (PHI). All PHESS hospitals use IPsec VPN for transmitting data to the receiving system. VPN connectivity simplifies communication between the sending and receiving applications because the two endpoints appear to be on the same network, eliminating the need for encryption because the VPN handles these tasks. The sending application connects to the receiving application using TCP on a specified port. Data that is exchanged between the two applications flows through the VPN tunnel and is automatically encrypted.

## **B. HL7 Interface Engine**

An Integration Engine coordinates and streamlines the exchange of messages between multiple healthcare applications, databases and systems, in any format, across virtually any platform. Hospitals send PHESS data in a standard HL7 ADT (“admit discharge transfer”) message to an external TCP listening application that receives HL7 messages on a pre-assigned port. The hospital interface queues messages on its integration engine and establishes a TCP connection to the remote listener. When a connection is established, messages are sent to the listener. The receiving application processes the message and sends an ACK/NACK to the sending application which serves as an indication for the sending application to send the next message in the queue. Most integration engines can create TCP listeners to receive messages from hospitals and confirm their receipt by sending an acknowledgement message to the sending application. A wide range of integration engines are commercially available for managing ADT message transactions.

## **C. Message Queuing/Processing**

After messages arrive at the integration engine, they are stored in a message queue where they are parsed and the payload data extracted. The payload data can then be processed in applications that will consume the clinical information, such as ESSENCE. Message queuing and processing functions can be performed within the interface engine or as an external application.

## **D. System Maintenance**

System maintenance can be divided into two categories. The first is daily monitoring. Because data flows can be unexpectedly interrupted for many reasons, operational data feeds must be continuously monitored. When data transmission rates fall below a pre-specified threshold, troubleshooting mechanisms are triggered. These mechanisms can include automatic stopping and restarting of network listeners, automatic notification of PHESS system engineer, and human intervention. Depending on the architecture of the collection system, automated troubleshooting mechanisms may be implemented

within the interface engine or as an external application. A second maintenance task relates to hospital reconnections. Connected hospitals periodically make modify their key system components, which may require reconfiguration (“reconnection”) efforts on the receiving end.

## ***II. Transition Strategies***

Pre-requisites for assuming operation of the collection system include securing appropriate resources (including personnel, hardware, and software) for establishing and maintaining secure network connectivity, message processing infrastructure, and data flow monitoring.

The ADT interfaces from INPC hospitals cannot be transitioned because 1) they are used for multiple purposes (including PHESS), and 2) contain additional information not specified in surveillance regulations. Consequently, the transition strategy for hospitals participating in the Indiana Network for Patient Care (INPC) differs from non-participating hospitals. The entities assuming operation of the collection system would need to either continue using the INPC or establish separate data feeds. Please see the “PHESS Project Plan Narrative” and “PHESS System Architecture” documents for additional details for each of the steps listed below:

### **A. Non-INPC hospital transition**

The following describes a transition strategy to be applied to each existing data flow for hospitals not participating in the INPC:

1. Establish contact with hospital networking and messaging personnel. (Existing contact information would be provided)
2. Coordinate with hospital source system personnel to re-build real-time, point-to-point IPsec VPN connections for each hospital source system. A hardware VPN solution (e.g. Cisco VPN concentrator) is recommended. Existing connection parameters will be provided.
3. Configure HL7 interface engine to accept, acknowledge, queue, and process real-time HL7 ADT data feed.
4. Test data feed from hospital source to receiving application.
5. Go-live after successful end-to-end testing; discontinue prior collection system; enter maintenance phase. General reconnection processes are covered below. Interface engine/message flow

monitoring and troubleshooting will be specific to hardware/software chosen.

## **B. INPC hospital transition**

The following describes a transition strategy to be applied to each existing data flow for hospitals participating in the INPC:

1. Establish contact with hospital networking and messaging personnel. (Existing contact information would be provided)
2. Coordinate with each hospital's IT personnel to build new real-time secure connections.
3. Iteratively review and validate HL7 messages to establish conformance with HL7 specification and surveillance regulations.
4. Configure HL7 interface engine to accept, acknowledge, queue, and process real-time HL7 ADT data feed.
5. Test data feed from hospital source to receiving application.
6. Go-live after successful end-to-end testing; enter maintenance phase. Interface engine/message flow monitoring and troubleshooting will be specific to hardware/software chosen.

## ***III. Maintenance Tasks: Reconnection Process***

As a part of system maintenance source system data flows must be reconfigured ("reconnected"). While specific reconnection scenarios will vary, this section describes common source system modifications and tasks necessary to reconnect hospitals.

### **A. Core source system components**

Modifications to any one of three key hospital source system components may require re-connection efforts. Modifications can be interdependent; that is, change to one component may require change to additional components. The three key source system components are:

**Patient  
registration**

When a patient presents to an emergency department (ED), patient registration captures the data elements necessary for surveillance, and is a core function in all hospital information systems.

**Messaging**

This subsystem is responsible for routing data both within a hospital and to outside recipients, and commonly uses a product called an ‘interface engine’.

**Network  
connectivity**

Network connectivity refers to the physical network (such as the Internet) and hardware supporting the network (routers, etc.) over which data is transmitted.

## **B. Common modifications**

Three common types of modification can occur with any of the three source system components. These changes include:

**Vendor change**

Organizations may transition from one manufacturer of a particular software or hardware product to another. For example, a hospital may transition from a Cerner system to a McKesson system.

**Version upgrade**

Software is routinely modified (“patched”) to add new features and fix known bugs, which can alter system functionality.

**Configuration  
change**



Software and hardware systems can be modified to function in a variety of ways. Evolving workflows, business logic, and functional requirements may require re-configuration of an existing system.

## C. Reconnection tasks

Table 1 represents a generalized 3x3 grid of nine common source system modifications. Following the table is a narrative characterizing the tasks associated with these modifications.

Table 1: Classes of source system modifications requiring reconnection. Letters in each cell represent sets of likely reconnection tasks, although specific reconnection scenarios will vary. Brackets indicate tasks that may not be required for each reconnect. Each letter refers to the following document subsections: D- Message review, E- Connectivity, F- Go-Live

	Registration	Messaging	Connectivity
<b>Vendor Change</b>	D,F	D,[E],F	E,F
<b>Version Upgrade</b>	[D],F	D,[E],F	[E],F
<b>Configuration Change</b>	[D],F	D,[E],F	[E],F

## D. Message Review

1. **Coordinate message review action items and schedule.** Data interface staff have limited availability because they serve a critical role in hospitals. Consequently, multiple communications are required to coordinate appointments and establish message review process.
2. **Provide HL7 Specification Guidance.** Technical information and guidance is provided to interface engineers who create a sample message set.
3. **Implement Test Message Listener.** Hospitals transmit data to a unique network TCP/IP port, called a "test listener". The listener is implemented to temporarily receive sample messages for review prior to going live.
4. **Analyze Sample Messages.** Messages reviewed for completeness of data and compliance with HL7 standard. Messaging engineers review sample HL7 messages for non-standard formatting and also for missing or misplaced data elements. The result of this review is a summary analysis with recommended changes to the messages.

5. **Provide Message Analysis Summary.** We provide a summary message analysis to the hospital for their review. The summary analysis serves as a guide to assist hospitals with modifications to their messages. Reviewing messages and recommending changes is an iterative process and can require more than one review-update cycle.
6. **Certify messages as finalized.** Once the messages are verified to comply with the HL7 specification, and contain the data elements required for PHESS, the iterative message review is complete, and messages are certified as being complete and compliant with HL7 standard.
7. **Modify Production Message Listener.** The unique hospital identifier in each HL7 message may change and require re-configuration in the message listener. Hospitals transmit data to a unique network TCP/IP port (called a "listener"). These unique numbers are negotiated with each hospital to fit within their existing network policies, and may change with reconnection.

## **E. Re-establish Connectivity**

1. **Coordinate connectivity action items and schedule.** Network staff has limited availability because they serve a critical role in hospitals. Consequently, multiple communications are required to coordinate appointments and establish re-connection process.
2. **Identify connectivity hardware/software configuration changes.**  
Secure network connections are created using a variety of protocols and hardware. Though most hospitals favor IPsec VPN connections using Firewall or VPN concentrator technology, upon system change we must verify the connectivity protocol in order to direct the connection process. Identifying the equipment vendor and software improves process efficiency by highlighting any known incompatibilities between different equipment vendors.
3. **Provide VPN connectivity worksheet.** Secure network connections are created using multi-step-protocols. Several pre-specified configuration parameters must be agreed upon by the network end-points before hand. We provide the hospital with a customized VPN connectivity worksheet with pre-specified parameters to guide the reconnection process.

4. **Configure VPN connection.** After the secure connection protocol and hardware/software specifications are finalized, the physical connection is established. During this process, we implement protocol-specific information necessary to configure the end-points with the connecting hospital. The physical connection is verified by successfully transmitting network packets from point-to-point. Time required for this task is highly variable due to many points of failure in the complex network protocols.
5. **Configure auxiliary network devices.** The source system (hospital) may have unique business logic that requires the receiving system (Regenstrief) to modify other network hardware in addition to the VPN concentrator. Although auxiliary route changes are most commonly made to our edge firewall, change to other network devices may be required.
6. **Configure Message Processor static routes.** The HL7 message processor sends acknowledgement of message receipt back to the hospital via a "static route". A change to network connection requires reconfiguration of the acknowledgement message static route.

## F. Go Live – Establish Data Transfer

1. **Coordinate go live schedule.** Once connectivity, messages, and message listeners are finalized, we negotiate a go-live date to test end-to-end data transmission from the source system, through the secure connection and onto the ISDH.
2. **Validate flow through message processing infrastructure without exception.** The systems engineer traces initial messages sent from a re-connected hospital from end-to-end to verify that messages are successfully delivered, and that no message exceptions are generated.

## Appendix A: Frequently Asked Questions

**What is a VPN?**

Short for virtual private network, a VPN is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

**How is a VPN created?**

To build a VPN tunnel between remote sites, specific hardware and knowledge of networking is required.

**What hardware is needed for building a VPN?**

To build a VPN tunnel, a VPN Concentrator or a VPN capable Firewall is recommended. Since a sending application must communicate with a receiving application, a LAN-to-LAN VPN tunnel is required to ensure persistent connectivity.

**What is a LAN-to-LAN VPN?**

A LAN-to-LAN VPN tunnel connects two remote networks over the internet and encrypts any data that flows through it. Unlike a VPN Client, a LAN-to-LAN VPN is persistent and does not require a user log in to start a session.

**What information must be exchanged to create a VPN?**

To build a LAN-to-LAN VPN, the following information must be exchanged:

- VPN Concentrator or Firewall's external IP address (Peer IP)
- Encryption Algorithms.
- Pre-shared Key
- IP Address of remote hosts (IP address of server on which the integration engines reside)

**What skills are required for setting up a VPN?**

A qualified Network Engineer experienced in routing and configuring VPN tunnels is highly recommended to ensure intelligent interaction with network engineers at the hospital. This person should be able to advise his/her counter part at the hospital during configuration and troubleshoot connectivity issues at both ends. Experience with connecting to different brands of VPN appliances is highly recommended.

**What is a Configuration Worksheet?**

To configure a VPN tunnel in an efficient manner, a VPN configuration worksheet containing necessary information to setup a tunnel should be exchanged with the network engineer at the hospital in order to minimize the time required during actual configuration. This also reduces confusion and prompts network engineers to get clarifications prior to scheduling a time for configuration.

**Why is an Integration Engine Useful?**

When hospitals send ADT data to an external entity, they usually send it to a TCP server application at a remote site that listens for HL7 messages on a pre-assigned port. The interface at the hospital queues up messages on its integration engine and tries to establish a TCP connection to the remote listener. When a connection is established, messages are sent to the listener. The receiving application processes the message and sends an ACK/NACK to the sending application which serves as an indication for the sending application to send the next message in the queue.

An integration engine offers the ability to create a TCP server application to receive messages from hospitals and confirm their receipt by sending an acknowledgement message to the sending application. Once messages arrive at the integration engine, they can be routed to applications that will consume the HL7 message, such as Essence.

**Are there any Integration Engines available commercially?**

A wide range of integration engines are available commercially that can be used to receive ADT data streams and process them for downstream applications.

## PHESS - TRANSITION PLAN

### **What are some benefits of an off-the-shelf Integration Engine?**

An out of the box Integration Engine will save time building interfaces to receive data from hospitals. Integration engines allow easy configuration of TCP listeners/servers that can accept HL7 data streams, validate and massage data and pass it to applications downstream. An off the shelf package minimizes the need for in house software development expertise.

### **What are the disadvantages of commercially available Integration Engines?**

Commercially available engines offer numerous features that are not relevant to the PHESS project. Since most of these additional features come standard with some of the popular integration engines, they also drive up the cost. Integration engines require considerable amount of knowledge to create, manage and troubleshoot interfaces, therefore in depth knowledge of the product is required which translates to several hours of training to develop skills for using the integration engine efficiently.

### **Can an Integration Engine be built in-house?**

Yes, with in-house software development experience and with experience in EDI, TCP listeners can be developed to receive and acknowledge data received from hospitals.

### **What are the advantages of developing interfaces in-house?**

Developing an integration engine in-house to configure interfaces allows an organization to focus on the primary task of receiving and acknowledging receipt of messages, thereby reducing the overall cost of implementation because features offered by commercially available integration engines that are irrelevant to the PHESS project need not be developed. Developing an integration engine in-house eliminates the need for waiting for an external resource to troubleshoot problems with interfaces, because troubleshooting can be done internally and can begin immediately upon first indication of any problems with an interface.

### **What are the disadvantages of developing an Integration Engine in-house?**

## **P H E S S - T R A N S I T I O N P L A N**


To develop robust interfaces, in depth knowledge of HL7 message processing, and experience in development of EDI applications is required. Considerable amount of time and money could be wasted in the process if the development team is not focused or experienced in developing and maintaining interfaces that need to be up 24/7. Loss of a key development resource during or after implementation can pose a great threat to long term maintenance of a system developed in-house.

### **What Skills are required to operate and maintain an Integration Engine?**

An interface programmer with knowledge of HL7 messaging protocols and experience in configuring, managing and troubleshooting HL7 data feeds.

## Appendix B: Sample VPN Worksheet

Sample worksheet used to collect information necessary to create VPN tunnels.

		<b>VPN Configuration Worksheet</b> <i>XYZ Hospital</i>	
<b>Contact Information:</b>		<i>ISDH / Vendor</i>	<i>XYZ Hospital</i>
<b>Technical Contact</b>			
Title:			
Phone:			
Fax:			
Email:			
<b>Support Contact:</b>			
Phone:			
<b>Network Information:</b>		<i>ISDH / Vendor</i>	<i>XYZ Hospital</i>
<b>VPN Unit WAN Interface</b>			
IP Address of firewall (Tunnel endpoint/Peer):		<external ip address>	
<b>VPN IKE Phase 1 Properties</b>			
Encryption Scheme:		IKE	
Key Exchange Method:		3DES	
Hashing Algorithm:		MD5	
Authentication Method:		<i>Will be disclosed at time of configuration</i>	
Aggressive Mode Support:		No	
Diffie Helmen Group for Phase 1:		Group 2	
IKE SA (Phase 1) Lifetime		28,800 Sec	
<b>VPN IKE Phase 2 Properties</b>			
Encryption Scheme:		IKE	
Transform (IPSec Protocol)		ESP	
Encryption Algorithm:		3DES	
Data Integrity:		MD5	
Use Perfect Forward Secrecy (PFS):		No	
Diffie Helmen Group for Phase PFS:		Group 2	
IPSEC SA (Phase 2) lifetime:		28,800 Sec	
Key Exchange for subnets:		Yes	
<b>VPN LAN Connections (Hosts)</b>			
IP Address:		<ip address of host>	
Subnet Mask:		<subnet mask>	
TCP Port:		<tcp port number>	



